ATTACHMENT A

FILED ENTERED
LODGED RECEIVED

FEB 25 2020

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The residence located at 16103 NE 95th Ct., Redmond, WA 9805, et al., more fully described in Attachment A1-A4

Case No. MJ20-089

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

The residence located at 16103 NE 95th Ct., Redmond, WA 9805, et al., more fully described in Attachment A1-A4

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B1-B4, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
8 U.S.C. §§ 2261A; 876(c); 371	Stalking; Mailing Threatening Communications; Conspiracy

The application is based on these facts:

✓ See Affidavit of Special Agent Michael Stults continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Michael Stults, FBI Special Agent
Printed name and title

◉ The foregoing affidavit was sworn to before me and signed in my presence, or
○ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: February 25, 2020

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
Printed name and title

USAO# 2018R00225

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Michael Stults, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the FBI, currently assigned to investigate domestic terrorism in the Seattle Field Office and have been so employed for 2 years. My experience as an FBI Agent includes the investigation of cases where individuals frequently utilize computers and the Internet to coordinate and facilitate various crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment. I have received advanced training on network and information security, and on the methods and tactics of open source intelligence gathering.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the following:

a. The premises known as 16103 NE 95th Ct., Redmond, WA 98052, hereinafter "PREMISES," further described in Attachment A1, for the things described in Attachment B1.

b. 2006 Black Toyota Tundra, WA C70066N, hereinafter "VEHICLE," further described in Attachment A2, for the things described in Attachment B2.

c. Black ZTE Blade Force 4G N9517, Electronic Serial Number 256691624201282613 hereinafter "PHONE," further described in Attachment A3, for the things described in Attachment B3.

d. Storage unit #3348, within the Public Storage at 12425 NE 124th St., Kirkland, WA 98034, further described in Attachment A4, for the things described in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Attachment B4.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement personnel; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

4. As set forth below, I have probable cause to believe that the three locations to be searched will contain evidence of Title 18, United States Code, Sections 2261A (Stalking); 876(c) (Mailing Threatening Communications); 245 (Federally Protected Activities); and 371 (Conspiracy) have been committed by known and unknown persons.

APPLICABLE LAW

5. Title 18, United States Code, Section 2261A provides for criminal penalties for whoever:

> with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that--
>
> (A) places that person in reasonable fear of the death of or serious bodily injury to a person, . . . described in clause (i), (ii), (iii), or (iv) of paragraph (1)(A); or
>
> (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A).

6. The persons described "in clause (i), (ii), (iii), or (iv) of paragraph (1)(A)" are:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(i) that person;

(ii) an immediate family member (as defined in section 115) of that person;

(iii) a spouse or intimate partner of that person; or

(iv) the pet, service animal, emotional support animal, or horse of that person.

7. Title 18, United States Code, Section 876(c), provides for criminal penalties for:

Whoever knowingly so deposits or causes to be delivered as aforesaid, any communication with or without a name or designating mark subscribed thereto, addressed to any other person and containing any threat to kidnap any person or any threat to injure the person of the addressee or of another

8. Title 18, United States Code, Section 245 provides that:

Whoever, whether or not acting under color of law, by force or threat of force willfully injures, intimidates or interferes with, or attempts to injure, intimidate or interfere with— . . .

(b)(5) any citizen because he is or has been, or in order to intimidate such citizen or any other citizen from lawfully aiding or encouraging other persons to participate, without discrimination on account of race, color, religion or national origin, in any of the benefits or activities described in subparagraphs (1)(A) through (1)(E) or subparagraphs (2)(A) through (2)(F), or participating lawfully in speech or peaceful assembly opposing any denial of the opportunity to so participate . . .

(b)(2)(C) applying for or enjoying employment, or any perquisite thereof, by any private employer or any agency of any State or subdivision thereof, or joining or using the services or advantages of any labor organization, hiring hall, or employment agency

9. Title 18, United States Code, Section 371 prohibits conspiring to commit a federal offense, and taking an overt act in furtherance of the conspiracy.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUMMARY OF PROBABLE CAUSE

A. Overview

10. The FBI has been conducting an investigation into Cameron Brandon Shea, formerly Cameron Brandon Chang, an individual living in Woodinville, Washington. Shea is a high-level member and primary recruiter for the Atomwaffen Division (AWD). AWD came to the attention of law enforcement on or about May 12, 2017, when Devon Arthurs was arrested for murdering two of his roommates near Tampa, Florida. Arthurs had been a member of AWD, as were his roommates. After his arrest, Arthurs admitted to the murders of his two roommates and told investigators he had committed the murders after he had converted to Islam and that the murders were his attempt at keeping the members of AWD from committing planned acts of terror related to the group's ideology. Arthurs claimed AWD had plans to use explosives to damage infrastructure and to commit acts of violence.

11. After Arthurs' arrest, another roommate, Brandon Russell, who was the leader of AWD, was encountered by law enforcement at the residence unharmed. In the residence, law enforcement found bomb-making precursor chemicals and hexamethylene triperoxide diamine, a high explosive chemical. Russell admitted the chemicals were his and, on or about May 20, 2017, Russell was charged in a federal criminal complaint in Florida with a violation of Title 26, United States Code, Section 5861(d) (possession of an unregistered destructive device) and Title 18, United States Code, Section 842(j)(unlawful storage of explosive material). In addition to the explosive material found inside the residence, law enforcement discovered Nazi paraphernalia, texts popular with neo-Nazis including Adolf Hitler's *Mein Kampf* and *The Turner Diaries*, and, among other things, a framed image of the Oklahoma City bomber, Timothy McVeigh, featured prominently in Russell's bedroom.

12. Following the arrest of Russell, AWD selected John Denton, a resident of Houston, Texas, and Kaleb J. Cole, aka Khimaere or Khim, formerly a resident of Arlington, Washington, to co-lead AWD in Russell's absence. Members of AWD also formed a relationship with Denver, Colorado resident, James Mason, who is the writer of the book, "Siege," which serves as the basis for AWD ideology. The book, which is a collection of neo-

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Nazi newsletters authored by Mason, advocates the leaderless resistance and lone offender strategies as a viable means to accelerate the collapse of the United States Government, which members of Atomwaffen Division believe to be controlled by Jews and other minorities.

13. On January 25, 2018, AWD hosted a "Death Valley Hate Camp" in Las Vegas, Nevada, where members trained in hand-to-hand combat, firearms, and created neo-Nazi propaganda videos and pictures of themselves posing with weapons. Cole coordinated the camp, beginning planning in early October 2017. Cole traveled from Washington State to Las Vegas for the hate camp with another AWD member, Aidan Bruce-Umbaugh. The two possessed concealed pistol licenses and transported numerous firearms and cases of ammunition to the event. California AWD member Samuel Woodward was expected to be at this hate camp, but could not attend due to being arrested for the murder of an openly gay Jewish college student.

14. Prior to YouTube removing their pages, AWD posted propaganda videos on two channels called "AWDTV" and "Atomwaffen Division." One of those videos titled "Zealous Operation," depicts a hate camp at Devil's Tower, an abandoned cement factory in Concrete, Washington. Approximately half a dozen AWD members can be seen wearing military style clothing, face masks, and carrying an assortment of long guns, while conducting paramilitary style training and shooting at a gravel pit attached to Devil's Tower. At the beginning of the video participants state, "*GAS THE KIKES! RACE WAR NOW*!" while the statement is spelled out at the bottom of the screen.

15. On February 23, 2018, *The Seattle Times* published an article discussing AWD, and identifying several of its members nationwide, to include some in Washington State. Photographs, along with personally identifiable information, including home and work addresses, were included in the article. The article also discussed the application Discord that members used to facilitate communication. According to the article, several thousand pages of Discord chat logs between members were hacked and leaked to the public. After having been identified, several of the AWD members, to include those in leadership positions, deleted their online profiles, quit their jobs, changed residences, and moved to the Swiss-based, encrypted

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

electronic communication service Wire, in an attempt to go dark and avoid detection by law enforcement. Cole was one of the AWD members identified in this article, but Shea's involvement in the group was not reported.

16. [redacted] on or about September 16, 2018, Cole posted a recorded leadership message to AWD members via Wire. In the recording, Cole said, "*The matter of these nosy reporters coming into our daily lives, where we work, where we live, where we go in our spare time. We must simply approach them with nothing but pure aggression. We cannot let them think that they can just... that that it's safe for them to just come up to us, and fuck with us. We cannot let them think they are safe in our very presence alone....*"[1] The statement was in response to an incident where a journalist confronted Denton at a music festival in Texas for the "*Documenting Hate*" news series.

17. Investigation into the group had identified Krokodil as a Washington based member who was the primary recruiter for AWD. Krokodil was also active in other online forums such as Gab and FascistForge.com, where he espoused racial violence, and stated how he and other members could "*go full McVeigh and start dispatching political and economic targets today, helping build the social tension that will accelerate the collapse of the system.*" Krokodil had also been planning to attend a November 2018 AWD Hate Camp being held in western Washington State, but was ultimately unable to attend due to medical reasons. Investigation later positively identified the user of the Krokodil moniker was Shea based on physical surveillance, consensual video recordings, and records demonstrating ownership of his phone number.

18. On July 9, 2019, Cole was interviewed by the FBI when he was deported from Canada to the United States. During the interview, Cole blamed the media for sensationalizing information about AWD and expressed dismay as to why he was targeted by the media in their stories, and lamented how he was never approached in an attempt to collect accurate information. Cole felt the media's reporting of AWD being a threat to the public was "*internet*

[1] [redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

nonsense."

19. In August of 2019, leadership members of AWD attended a "Nuclear Congress" in Las Vegas, Nevada, where members gave presentations, discussed recent events, challenges, plans going forward, and operational security. Shea discussed the importance of keeping identity protected, and how the media continues to be a challenge to AWD.

20. On September 26, 2019, Cole was served with an Extreme Risk Protection Order (ERPO) by the Seattle Police Department (SPD). SPD and Arlington Police Department officers seized 9 firearms in Cole's possession, as well as a number of unfinished lower rifle receivers, capable of being milled into functional rifle components with the equipment Cole owned. In the wake of the ERPO service, several news outlets nationwide covered the event. [redacted] covered Shea, Cole, and other AWD members discussing and disparaging the media coverage of the event, with one member suggesting to "*hit back... embarrass the enemy on their own front.*" Cole then left Washington State and resettled in Texas.

21. On November 4, 2019, Cole and Bruce-Umbaugh were stopped by law enforcement for speeding in Post, Texas while on their way to meet with Denton, near Houston, Texas. Bruce-Umbaugh was subsequently arrested for 18 USC 922 (g)(3) (Possession of a Firearm by an Unlawful User of a Controlled Substance). Law enforcement seized four firearms and approximately 2000 rounds of ammunition. Cole continued to the Houston area to meet with Denton.

B. Operation Erste Säule

1. The Planning

22. [redacted], in or about November 2019, Shea, using the moniker Krokodil, participated in a private Wire chat group titled, Operation Erste Säule.[2] Shea invited coconspirators to this chat group to collaborate and coordinate an effort to deliver threatening messages to journalists' homes and media buildings. Shea described the Operation in a message to the chat group: "*We're coordinating this nation wide Operation called Operation*

[2] Based on publicly available translation services, "Erste Säule" translates from German to English as "First Pillar."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Erste Säule, named after the first pillar of stat[e] power, AKA the media. We will be postering journalists houses and media buildings to send a clear message that we too have leverage over them . . . The goal, of course, is to erode the media/states air of legitimacy by showing people that they have names and addresses, and hopefully embolden others to act as well."[3]

23. Other participants in the Operation Erste Säule chat group included Cole (then based in the Houston, Texas area who used Wire name "पकजबतचषथबल"); an individual in the Cleveland, Ohio area who used Wire name "14ALG88"; Taylor Ashley Parker-Dipeppe, an individual who lives in Florida and used the Wire name "Azazel"; an individual in California who used Wire name "OldScratch"; Johnny Roman Garza, an individual in the Phoenix, Arizona area who used the Wire name "Roman"; an individual in Florida who used the Wire name "Lazarus", an unidentified individual believed to be in Oregon using Wire name that appears as "☒☒☒☒☒," an individual in South Carolina who used the Wire name "Swissdiscipline," and others.

24. Based on a review of the group's Wire chats, Cole and Shea were the primary organizers for Operation Erste Säule. Cole had access to the entire target list, helped to develop threatening posters to leave at the victims' homes, and made suggestions to Operation Erste Säule coconspirators on who to target, how to find people's home addresses, and, among other things, how to film the Operation when it happened. Shea, in addition to announcing the Operation, coordinated its various stages, including address collection, poster creation, and ultimate execution.

25. As part of Operation Erste Säule, each participant was directed to identify, research, and locate journalists in their area. "OldScratch" recommended using the website https://www.spj.org/fdb-list.asp to pick targets; that website is for the Society of Professional Journalists and contains a list of journalists and their contact information. "Lazarus" reported that he had three targets, and one was Jewish. "14ALG88" advised he was targeting three Jews. Garza said he had found "*a leader of an 'association of black journalists'*" in his state.

[3] [redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Shea stated that the identification of these targets was "*Excellent work!*" and "*Outstanding.*" Similarly, Cole said "*NICE WORK*" when he learned that "14ALG88" had found the addresses for three Jewish journalists. In addition, at one point in the group chat, Cole wrote that Atomwaffen Division members in Washington, Oregon, California, Ohio, and Florida, had acquired addresses to target during the campaign.

26. On or about December 11, 2019, during a discussion to coordinate Operation Erste Säule, Shea explained that he wanted to coordinate the Operation on the same night so journalists would be caught off guard, and to accomplish an effective "*show of force, demonstrating we are capable of massive coordination.*" Garza said that the intended impact of the coordinated Operation was to "*have them all wake up one morning and find themselves terrorized by targeted propaganda.*" Cole also suggested buying rag dolls and knives so that participants could leave a doll knifed through the head at their target locations.

27. On or about December 11, 2019, during a Wire discussion to coordinate Operation Erste Säule, Cole reminded the coconspirators to film their execution of the Operation: "*so when you guys film clips for this project: Be sure to film your clips horizontally (landscape),* not *vertical (portrait).*" Based on my training, experience, and this investigation, I know that cellular telephones are capable of making video recordings using built in cameras, and that cellular telephones can be rotated to film vertically or horizontally.

28. On or about December 11, 2019, during a Wire discussion to coordinate Operation Erste Säule, Cole told his coconspirators that the group was working on getting more addresses and the posters. Cole suggested that his coconspirators conduct reconnaissance of their victims' addresses and suggested searching their addresses in Google maps. Cole told his coconspirators to use, "*proper electronic opsec measures,*" which I believe describes an effort to anonymize or privatize online actions to obfuscate activity and avoid law-enforcement detection.

29. On or about December 18, 2019, during a Wire discussion to coordinate Operation Erste Säule, the coconspirators discussed how to print the propaganda posters. "14ALG88" said that he may have trouble printing the posters at the library and Cole told him

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

to consider buying a cheap printer on Craigslist. Shea added that printers cost as little as $20 or $40. Garza emphasized that, "*[t]his Operation does deserve a decent printer.*" During this conversation about printing the threatening posters, Cole cautioned everyone to "*be sure to ONLY print in black and white*" to avoid leaving evidence behind. Cole explained: "*make sure everything is printed in black and white, so metadata won't show up (the tiny yellow dots that indicate information about the printer.*"

30. Later, "Old Scratch" told the Wire group that one of his targets was very far from him and that he was considering mailing the threatening posters, "*if that's acceptable.*" Garza added that his targets were also far away and, in an apparent reference to the infamous Unabomber, that the "*mail idea should not be wasted . . . Unapropagandist.*" Shea emphasized operational security to anyone who decided to mail the threatening posters in order to avoid detection by the FBI. Specifically, Shea told his coconspirators to "*buy your stamps in another town with cash while wearing a disguise lol[.] And utilize a mailbox with no cameras nearby, post office = big no no[.] And wear medical gloves when handling all materials, make sure both the destination and return address (if you're dumb enough to add one) are printed on paper and cut out + taped onto envelope, no hand writing allowed.; when sealing the envelope, use a q-tip dipped in water instead of your tongue, unless you want the FBI to have your DNA.*"

31. On or about December 25, 2019, during a Wire discussion to coordinate Operation Erste Säule, Cole explained that he was going to distribute the threatening posters via "Guerrilla Mail" with the subject line, "*prop-run.*" Guerrilla Mail is an electronic communication service accessible via internet-connected devices that offers temporary, disposable e-mail accounts. On or about December 26, 2019, Cole confirmed via Wire that everyone involved in the Operation had received their propaganda poster. Around the same time, Parker-Dipeppe confirmed that he and "Lazarus" were working together, with "Lazarus" as the leader and Parker-Dipeppe as the "*second.*" Then, Garza asked when they were going to execute the Operation. Over the next week, Shea, Cole, Garza, "Lazarus," Parker-Dipeppe, "Old Scratch", "☒☒☒☒☒," and others continued to coordinate a date to execute Operation

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Erste Säule. Ultimately, the participants agreed to carry out the Operation on January 25, 2020.

32. On or about December 27, 2019, Garza told the group via Wire that he was, "*scoping my places on maps right now*." That prompted a conversation among the coconspirators about avoiding detection when executing the Operation. Garza suggested using a disguise to blend into the neighborhood, such as wearing construction gear or posing as a "*mail deliverer,*" or to execute the Operation at night. As for targets in gated communities, Garza suggested "*check[ing] it out irl [in real life] or on the maps, you should be able to spot mounted cameras. If they aren't around the gate then its almost no big deal to find a wall to hop.*" Shea added that he planned to use a bicycle instead of his car to approach his targets in order "*to avoid license plate captures*." During a later chat, Shea warned his coconspirators to be careful and look for any security cameras, and Parker-Dipeppe advised, "*Be very cautious of the surrounding and use google maps if possible to search around.*"

33. On or about January 6, 2020, during a Wire discussion to coordinate Operation Erste Säule, the coconspirators again coordinated the Operation and exchanged opinions about whether to conduct the Operation entirely via the mail, rather than in person. Ultimately, the coconspirators decided to stay with "*boots on the ground*" at some locations, while mailing the threatening posters to the riskier target locations, as shown in the below exchange:

"Lazarus":	Hm Well it's less threatening if we just mail them.
Parker-Dipeppe:	Honestly not a bad idea but I like the dangerous side more
"Lazarus":	But I do see the whole safety thing[.] I say, the night of posters before we put up any we check the house for security and etc, if the house has to much security we mail them but if it doesn't have a lot and we can get by with our masks then we put the posters up

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Shea:	What I don't want happening is one of you boys being caught, that's my main concern
"Lazarus":	We know, but you also have to understand we all know what we signed up for[.] So I say we go threw with the plan but if a house has to much security we mail that poster to that house.
Parker-Dipeppe:	It will look suspicious especially on me and Lazs end driving with a New Jersey plated car and parking somewhere random[.] However we've gotten away with it in the past too.
	. . .
"Lazarus":	… Worse case we mail the poster[.] My point is if we want to send a message it would look better if we put that poster up[.] Mailing them yes seems effective enough, but it doesn't send a bigger and greater message then actually putting up a poster at someone's house
Parker-Dipeppe:	Agreed
Garza:	I think the locations with the most possible security concerns could be mail targets, but those locations that look much less secure can be visited . . . It's not like they're expecting us in person. If they all receive some shit in the mail consecutively, it'll draw the same stir. Maybe not as novel as a physical visit with a poster on their front window, but in the 'scare range' just the same.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Shea:	Seems like a good plan, then. Greater security = mail, less = poster.
	. . .
"☒☒☒☒☒":	One of my locations is the headquarters of the new station in my city, so I should mail it yeah? I could add some 'personal' touches to make it special.
	. . .
Shea:	News station? You could mail it or post it up. I'd say posting it on public establishments is less risky than houses.
"☒☒☒☒☒":	Got it

34. On or about January 7, 2020, Shea addressed the illegal nature of the Operation and told his coconspirators via Wire: "*If we are arrested later in connection to the Operation, but they can't prove we specifically did it, fedwaffen's open sourcing of the AW brand name gives us plausible deniability...And since we have JM's [Mason] disavowal of fedwaffen on the website, saying we disavow illegal action, that further helps our point that fedwaffen was behind this.*" As part of its investigation into Atomwaffen Division, the FBI knows that "fedwaffen" is a reference to a faction of unknown individuals who have, in recent months, posted Atomwaffen Division videos and propaganda online claiming to be Atomwaffen Division. Mason and members of the real Atomwaffen Division, however, have disavowed this new unsanctioned faction and all its communications.

35. As described above, Cole has mentioned multiple times during the Wire chats for Operation Erste Säule that he was designing and creating the threatening posters that the coconspirators would use. For example, Shea told the coconspirators that Cole "*is developing a number of posters that are threatening but not explicitly.*" And, over the course of multiple days, Cole stated he planned to "*finish up the posters here sometime tomorrow*," then "*okay*

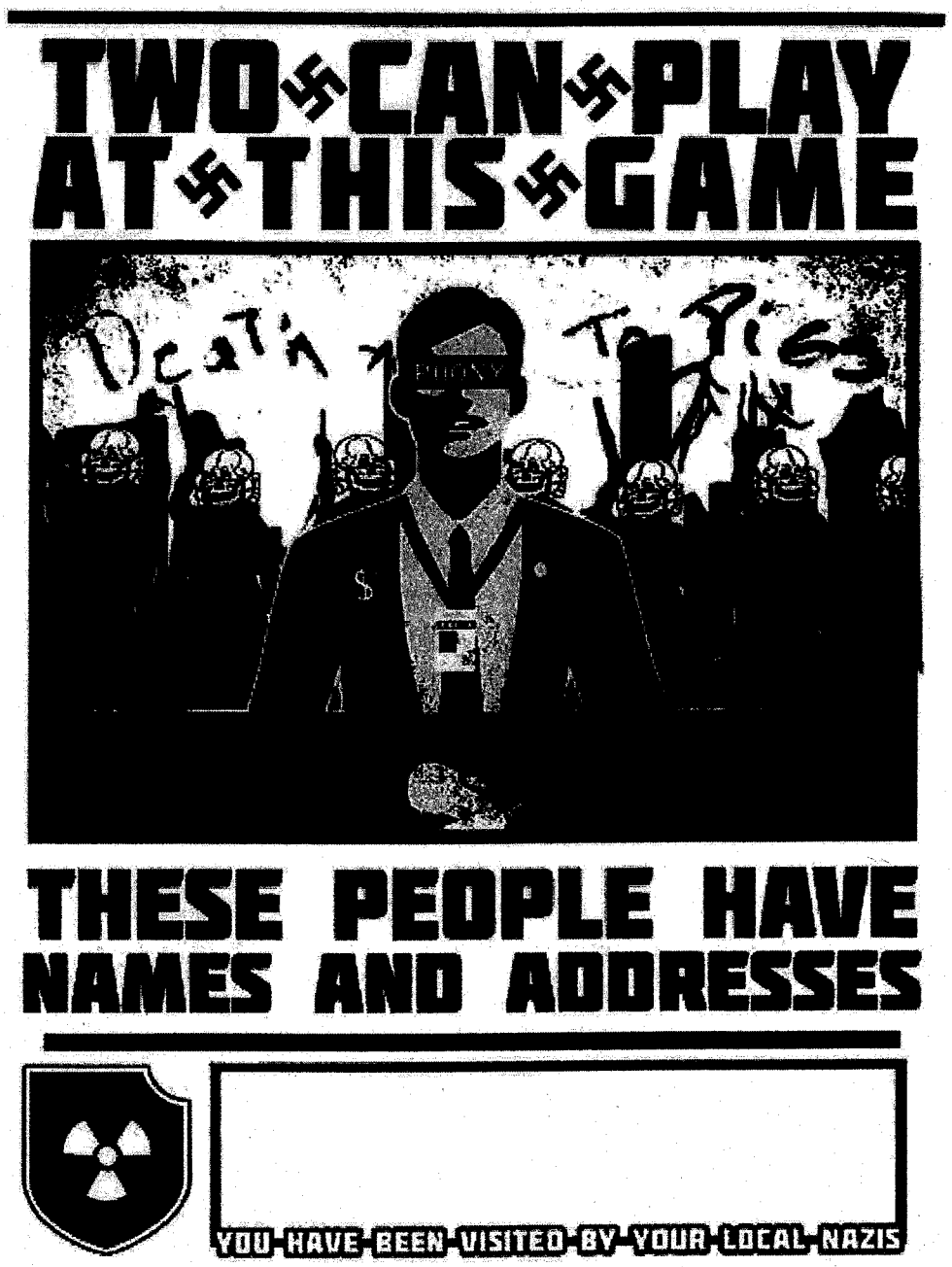
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

guys, I have finished the bulk of address posters," and, finally, that he had "*sent the posters out*" to coconspirators' e-mail addresses. When talking about the posters, Cole added that he had been "*having issues with my linux machine.*" Based on my training and experience, I understand a "linux machine" to be a personal computer using the linux operating system.

36. As part of this investigation, the FBI has obtained the draft posters that Atomwaffen Division considered using during Operation Erste Säule. All of the posters contain threatening statements and insinuations, indicating that the targets are under surveillance and at risk from Atomwaffen Division, and the draft posters contained a blank area at the bottom designated for the coconspirators to add a victim's address. Based on the group's own statements, Cole's prior statements about media intimidation, and the nature of Operation Erste Säule, I believe that the coconspirators intended for the following posters to intimidate, threaten, and cause substantial emotional distress to the group's targets.

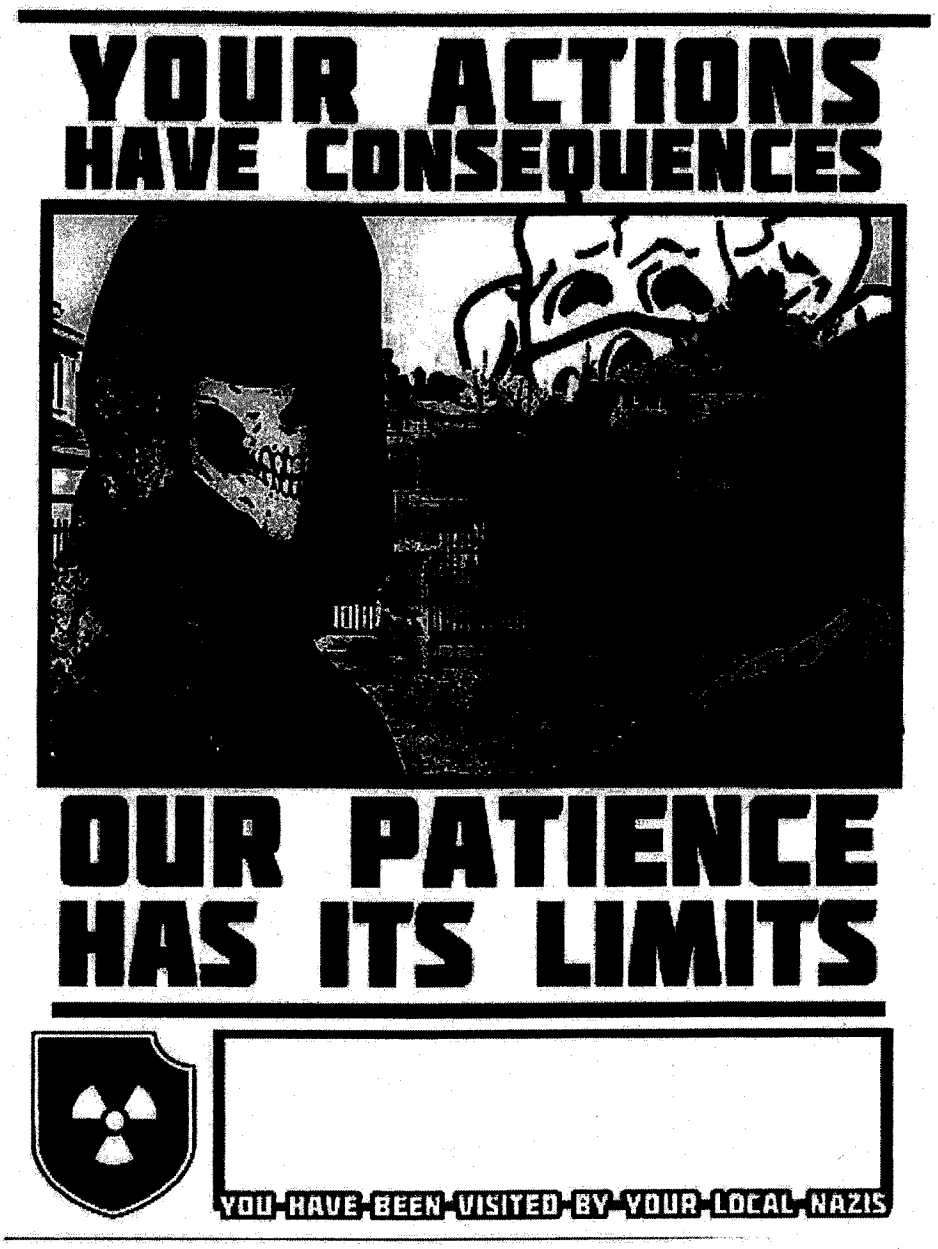
37. One of the posters features four swastikas, a drawing of a person with press credentials around his neck, anonymous figures behind him holding guns, and it says, "Death to Pigs," "Two can play at this game," "These people have names and addresses," and "You have been visited by your local Nazis."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



38. Another poster shows an anonymous figure wearing a mask and holding a Molotov cocktail, and it says, "Your actions have consequences[,] our patience has its limits" and "You have been visited by your local Nazis."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



39. Another features three swastikas and says, "We are watching[.] We are no one[.] We are everyone[.] We know where you live[.] Do not fuck with us[.]" At the very bottom of the poster are the words "You have been visited by your local Nazis."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

40. At various points during the Wire chats for Operation Erste Säule, the Atomwaffen Division coconspirators described why they want to carry out the planned campaign of threats. Shea told coconspirators that Cole was making posters designed to be "*threatening, but not explicitly.*" Later, Garza told the group, "*I believe that if we smash this, we can reap the reward of a nationwide scare,*" to which "Old Scratch" responded, "*Damn right bro.*" Garza also said that the Operation will "*have them all wake up one morning and find themselves terrorized by targeted propaganda.*" And, among other things, Cole said the campaign was to "*intimidate*" and make journalists fear Atomwaffen Division: "*if there isn't*

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

any coverage[] its because they don't want to bring more heat upon themselves, or fellow journos. aiding to their fear of us."

41. On or about January 22, 2020, Shea informed all participants of the Operation Erste Säule chat group that the Wire chat would be ending soon. In response, Cole stated: "*All I can say is get a few good video clips if you can.*" Finally, Shea reminded everyone to avoid getting caught, and suggested that if they did get caught to plead the Fifth Amendment and remind their lawyers of the "fedwaffen" defense described above. The Wire chat group then closed.

2. The Events in Washington State

42. On January 25, 2020, law enforcement conducted surveillance of Shea and observed him driving his vehicle to Redmond, Washington, and park in a Target parking lot. Shea then changed into a grey hoodie, stocking cap, and a surgical facemask. Shea proceeded to walk across the street into a Fred Meyer store where he purchased a book of Santa Claus stamps and packaging tape with cash. Based on my training, experience, and knowledge of the investigation, I believe Shea was obfuscating his appearance, consistent with the operational security measures mentioned above.

43. On January 29, 2020, the FBI was contacted by [redacted], a Seattle reporter who has reported on AWD, and [redacted], [redacted] of the Anti-Defamation League's Pacific Northwest Regional Office.[4] Both had received posters in the mail. [redacted] received the poster that is titled, "Two Can Play At This Game," and included [redacted]'s name, his home address, and his cell phone number. [redacted] received a poster titled, "Your Actions Have Consequences," and included [redacted]'s home address. The envelopes in which the posters arrived were both addressed by affixing cut-out, printed addresses with packaging tape, akin to the procedure Shea described in above in paragraph 26. The envelopes also both included Santa Claus stamps.

[4] The Anti-Defamation League's mission is to combat anti-Semitism and other forms of hatred and bigotry.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

44. On February 5, 2020, the Seattle Police Department was contacted by [redacted], who was formerly employed [redacted] of the Anti-Defamation League's Pacific Northwest Regional Office. [redacted] had recently returned from vacation when she opened her mail, and received the poster titled, "We Are Watching" which included [redacted]'s name and address at the bottom. The envelope the poster arrived in was postmarked January 27, 2020, and was mailed with a Santa Claus stamp.

3. The Events in Florida

36. On January 24, 2020, law enforcement conducted surveillance of Taylor Ashley Parker-Dipeppe, who agents had previously identified as being Azazel. Agents observed Parker-Dipeppe leave his residence in a white 2014 Hyundai Accent. Parker-Dipeppe traveled with a female and was wearing a black t-shirt, jeans, and boots.

37. The two arrived at a Goodwill Springhill Super Store in Spring Hill, Florida. They purchased a tan baseball hat, a hooded sweatshirt, yellow in color with what appeared to be black lettering on the front, and a pair of black sunglasses. The two then visited the Spring Hill Walmart. They purchased a pack of Gorilla Tape mounting tape squares. Parker-Dipeppe paid for both transactions using a debit card ending in 9799.

38. On January 25, 2020, Parker-Dipeppe and the female were observed leaving the residence above at approximately 8:30 p.m. They drove towards Tampa and arrived at an apartment complex in Tampa. Parker-Dipeppe dropped off the female and picked up a male in Saint Petersburg, Florida.

39. Agents observed Parker-Dipeppe and the male entering a Saint Petersburg Walmart late in the evening. The male purchased a TT sweater and black Avia pants. Both Parker-Dipeppe and the male exited the Walmart and then drove back to Tampa.

40. Agents then observed Parker-Dipeppe and the male drive to a Tampa residence. The two affixed a poster to the front of the residence, immediately below a bedroom window. The two then ran back to their vehicle and drove away. The poster had been affixed using mounting tape squares, *i.e.*, the same type of tape that Parker-Dipeppe had purchased at Walmart.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

41. The poster was the "We Are Watching" poster that is identified above. The poster included the name and home address of [redacted], a Florida news reporter who was born and raised in Puerto Rico.

42. [redacted] did not live at the residence. It appears that Parker-Dipeppe and the male had the wrong address. [redacted], who is black, lived at the residence with her father and minor child. [redacted] saw the poster.

4. The Events in Arizona

43. On January 25, 2020, law enforcement conducted surveillance of Johnny Roman Garza, also known as Roman, in the Queen Creek, Arizona area. Garza was picked up by an individual in a maroon Ford Taurus. Shortly after midnight, the vehicle was parked near an apartment complex in Phoenix, Arizona where a member of the Arizona Association of Black Journalists resided. At least one of the vehicle occupants exited the vehicle. The occupant returned to the vehicle, and the vehicle proceeded to the residence of an editor of a local Jewish publication. Both Garza and the other individual were observed fleeing from the direction of the residence to the vehicle. The two left the scene, and the individual dropped Garza off at his residence.

44. The editor found a poster titled, "Your Actions Have Consequences" that included the editor's name and home address at the bottom. The poster was glued to a bedroom window, on the north side of the editor's home.

C. Shea's Involvement and Use of the RESIDENCE, VEHICLE, and PHONE

45. As discussed herein, the FBI, through its investigation, has identified numerous members of Atomwaffen Division, including Shea, who have planned and conspired to implement a targeted campaigned with the goal of terrorizing journalists and Jewish community leaders with threatening propaganda.

46. Through the investigation, Shea was identified as the leader of the operation, who was actively aware of, and participating in all communication and planning leading to the execution of their plan. Shea's involvement includes:

a. On or about December 4, 2019, Shea, using his online moniker

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

"Krokodil," created the "Operation Erste Saule" private chat group in the WIRE application. Shea then invited several other AWD affiliates into the private group. The chat group was established and utilized for the planning and coordination of executing the targeted propaganda campaign. Based on my training and experience, I understand the Wire application is an internet-based application that can be utilized from an individual's cell phone or computer.

b. A main element of the operation was the identification of and research into the personal identifiable information of journalists in a member's respective area using a variety of online databases and open source information. Additionally, members including Shea, advocated for and discussed the usage of other internet-based resources to research and plan the operation such as querying security camera systems in order to familiarize themselves with the types of home surveillance available, what they look like, and any possible weaknesses they may have. Based on my training and experience, someone conducting internet research would need to utilize an internet connected device such as a phone or computer. Evidence of their internet activities, including search history and downloads, would likely be stored locally on any such device

c. The posters utilized in this operation were digitally created and personalized by inserting the recipients' information into the design. I understand that a computer program is required to make the observed graphic design and personalization. Such a program would require a personal computer to facilitate. Furthermore, the posters were then disseminated to co-conspirators via email, which would require internet connected devices such as phones or computers to access.

d. As part of the operation planning, the group discussed how printing the posters on your own printers at home was the best option. When discussing this point Shea stated *"My printer was only $40."* Based on my training and experience, I believe a personal printer of that price range, would be a basic USB connected device, designed to plug-and-play with a personal computer. It is probable Shea possesses a personal computer he utilized in conjunction with this printer to receive, process, and produce his propaganda materials within

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the RESIDENCE.

e. Based on toll analysis and subpoena returns, Shea assumed ownership of an Android ZTE phone with an MEID of 256691624201282613/ IMSI of 310120254586077, known to be the PHONE. This model phone is an internet connected device and capable of utilize web-based communication applications such as Wire. Physical surveillance has several times observed Shea being a fervent user of his PHONE. Toll information provides logs of phone usage for calls and texts, and there are several instances in which Shea is observed utilizing his phone, in which no network calls or texts were made. Based on my training, experience, and familiarity with the case, I believe Shea utilized the PHONE to access the internet and other internet-based applications that were likely in facilitation of the operation, coordination with co-conspirators, and in planning or research of the crimes described above.

f. Shea had discussed in the planning stages of the chat how he would utilize the VEHICLE the evening of the operation. Shea utilized the VEHICLE to transport himself to and from the Fred Meyer on January 25, 2020, where he purchased materials in furtherance of the crimes enumerated herein. Based on my training, experience, and knowledge of the investigation, since Shea uses the VEHICLE as his primary source of transportation, making it likely he would have stored, transported, or hid instrumentalities of the his crimes within the VEHICLE, where evidence of it would still remain.

47. Through February 13, 2020, Shea was residing in an apartment with his girlfriend in Woodinville, Washington. According to statements made by Shea, he broke up with his girlfriend and has left the apartment. According to tracking data on Shea's phone, he spent the evening of February 13, 2020 in a motel near his employer in Kirkland, Washington. Since then, according to the tracking data, Shea has not returned to the apartment. Instead, he is residing with his parents at the PREMISES. Specifically, for each day since February 13, Shea has spent each night at the PREMISES, in addition to other time spent at the PREMISES. Physical surveillance has observed Shea's truck parked on the street outside of the Redmond, Washington residence. Open source records checks of Shea also indicate that the PREMISES is a recent and active household listing for him. However, postal records indicate that Shea is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

still listed as an individual who currently receives mail at the Woodinville apartment, and no forwarding address for him has been provided. Washington State driver's license information shows that Shea has not updated his current residence in over three years, and it still displays an even older residence at an apartment complex in Kirkland where Shea has not lived for almost two and a half years.

48. During the search, agents plan to search only the areas of the PREMISES that appear to be where Shea has access to and/or resides. In addition, agents will seize only those digital devices that appear to belong to Shea as opposed to his parents.

49. Shea has rented a storage unit at the Public Storage in Kirkland, Washington since October of 2017, *i.e.*, the storage unit that is described in Attachment A4. Phone location data and access records from Public Storage indicate that Shea visited his storage unit for over an hour on February 13 immediately after leaving the Woodinville apartment. Shea again visited his storage unit on February 14. He had not visited his storage unit since November of 2019 prior to the visits on February 13 and 14. Based on my training, experience, and knowledge of the case, it is likely that Shea moved out of the Woodinville apartment, stored some items at his storage unit, and is currently residing at his parents address in Redmond.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS OF DIGITAL DEVICES AT THE PREMISES

50. As described above and in Attachments B1-B4, this application seeks permission to search for records that might be found on the PREMISES in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

51. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

52. *Forensic evidence*. As further described in Attachments B1-B4, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

53. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

54. I know that when an individual uses a computer to commit stalking over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

55. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media*. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

SEARCH TECHNIQUES FOR DIGITAL DEVICES AT THE PREMISES

56. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

57. Because multiple people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review.

58. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the PREMISES that are capable of containing data or items that fall within the scope of Attachment B1 to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

59. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B1 to this Affidavit.[5]

60. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the PREMISES will not result in access to any data physically located elsewhere. However, digital devices or other electronic

[5] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

storage media at the PREMISES that have previously connected to devices at other locations may contain data from those other locations.

61. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

62. Searching the forensic images for the items described in Attachment B1 may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B1 to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

REQUEST FOR SEALING

63. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application, affidavit and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation and disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Disclosure of these materials would give the target of the investigation an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

64. Under the operational plan, agents intend to arrest Shea in the middle of the night as he exits his car on the way to work. I seek authorization to search the VEHICLE prior to 6:00 a.m., to avoid having to leave the car, which otherwise would be unattended, in the work parking lot until 6:00 a.m. to begin the search.

CONCLUSION

65. Based upon the information that has been uncovered during the course of this investigation, and on the advice, experience, knowledge of other agents and officers involved in this investigation, I believe these facts establish probable cause to search the locations identified in Attachments A1-A4 for the items described in Attachments B1-B4.

MICHAEL STULTS, Affiant
Special Agent
Federal Bureau of Investigation

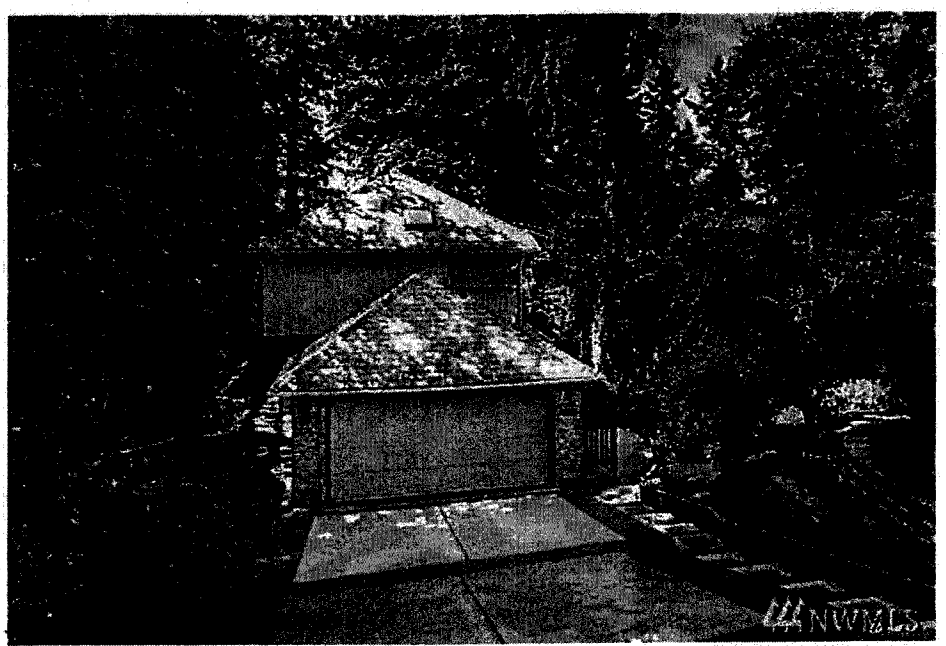
The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit on the 25th day of February, 2020.

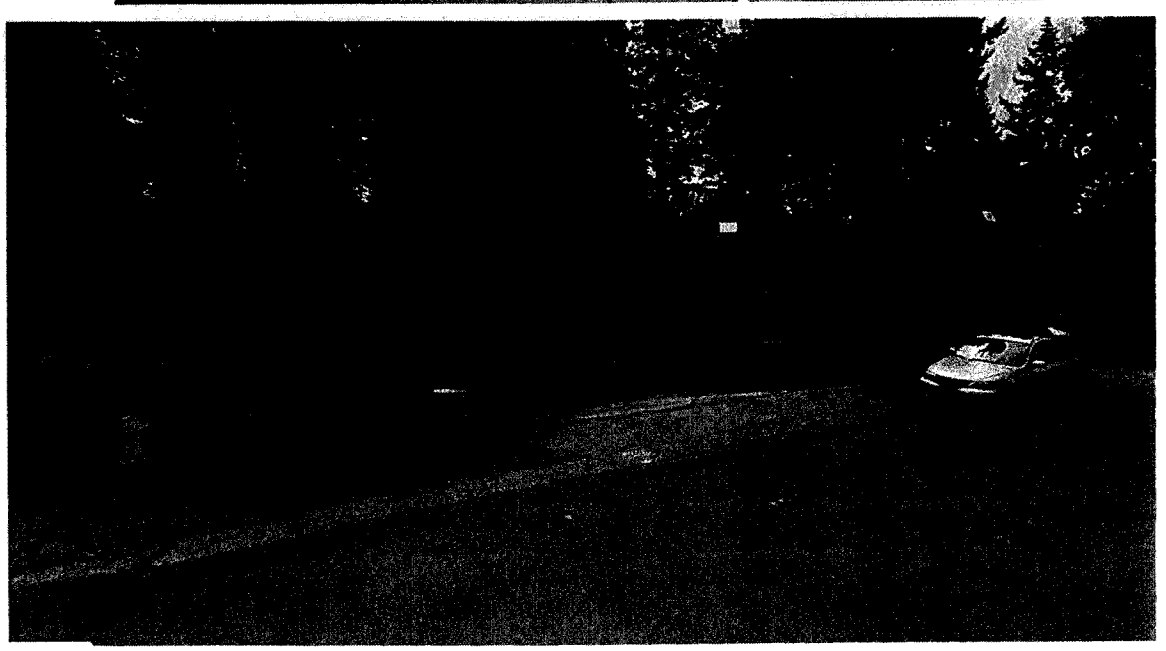
MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A1
Property to be Searched

The property to be searched is the residence located at 16103 NE 95th Ct., Redmond, WA 98052. It is a single family, two story home with a brick and beige exterior and grey roofing shingles. The number "16103" is visible to the right of the garage door which faces the street.





UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B1
Property to be Seized

Documents (in whatever form) relating to violations of Title 18, United States Code, Sections 2261A (Stalking); 876(c) (Mailing Threatening Communications); 245 (Federally Protected Activities); and 371 (Conspiracy), that is:

1. All documents relating to attempts to locate the home addresses of any members of the media, the Anti-Defamation League, persons who identify as Jewish, or ethnic minorities;

2. All documents relating to the Atomwaffen Division, including members of the group;

3. All documents containing swastikas, other Nazi symbols, or other symbology related to white-supremacist violent extremism;

4. All stamps, packaging tape, and blank envelopes;

5. All receipts reflecting purchases of stamps, packaging tape, or blank envelopes in January 2020;

6. All documents containing the monikers "Krokodil," "Lazarus," "14ALG88," "Azazel," "Roman," "Swissdiscipline," "OldScratch," or "पकजबतचषथबल";

7. All communications with Kaleb Cole;

8. Digital devices or other electronic storage media and/or their components, which include:

   a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

   b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

   c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

9. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media; and

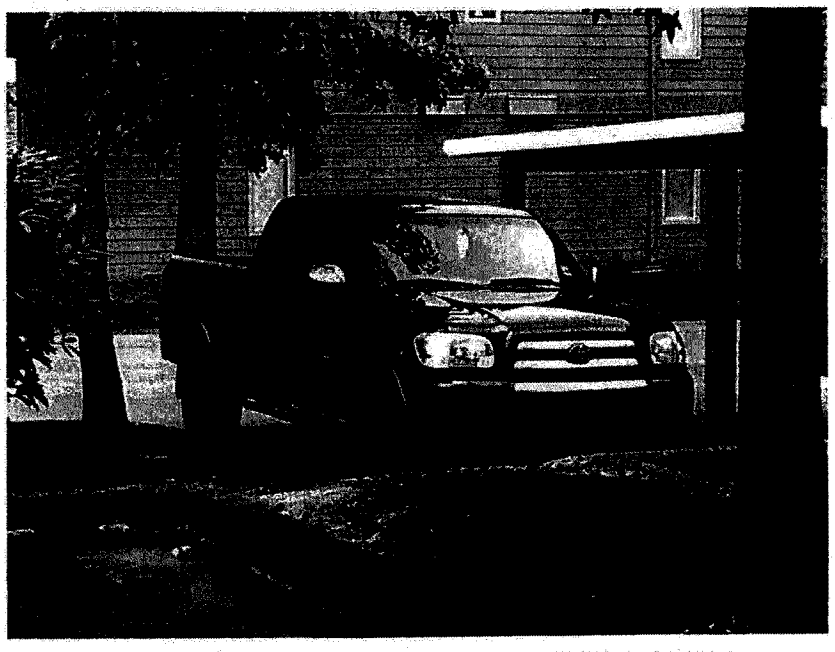
i. contextual information necessary to understand the evidence described in this attachment.

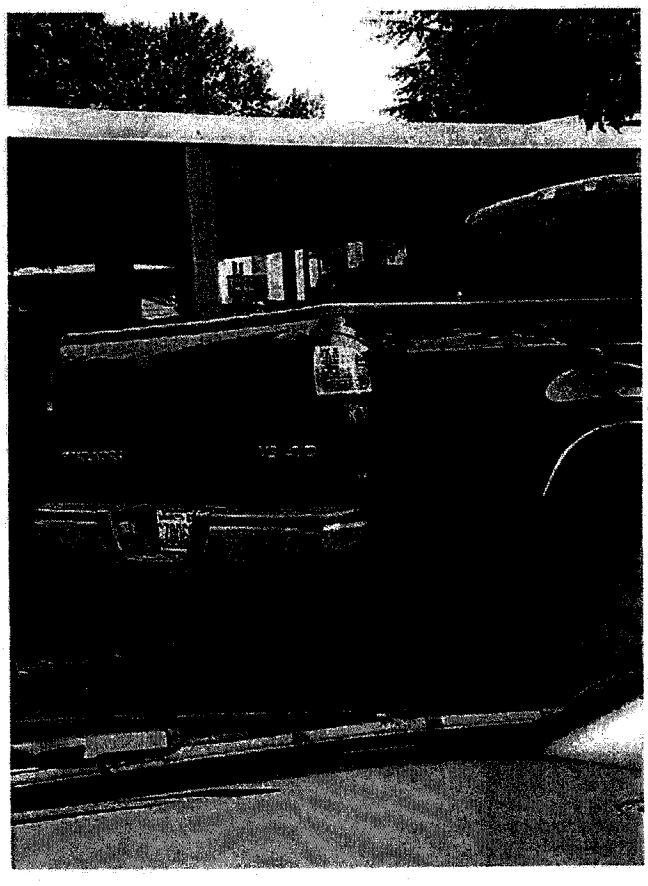
THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A2
Property to be Searched

The property to be searched is the 2006 Black Toyota Tundra, WA plate number C70066N.





UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B2
Property to be Seized

Documents (in whatever form) relating to violations of Title 18, United States Code, Sections 2261A (Stalking); 876(c) (Mailing Threatening Communications); 245 (Federally Protected Activities); and 371 (Conspiracy), that is,

1. All documents relating to attempts to locate the home addresses of any members of the media, the Anti-Defamation League, persons who identify as Jewish, or ethnic minorities;

2. All documents relating to the Atomwaffen Division, including members of the group;

3. All documents containing swastikas, other Nazi symbols, or other symbology related to white-supremacist violent extremism;

4. All stamps, packaging tape, and blank envelopes;

5. All receipts reflecting purchases of stamps, packaging tape, or blank envelopes in January 2020;

6. All documents containing the monikers "Krokodil," "Lazarus," "14ALG88," "Azazel," "Roman," "Swissdiscipline," "OldScratch," or "पकजबतचषथबल"; and

7. All communications with Kaleb Cole.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A3
Property to be Searched

The property to be searched is the Black ZTE Blade Force 4G N9517, Electronic Serial Number 256691624201282613.

Note: The image provided is a stock image of the device, not the actual device possessed by Shea.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B3
Property to be Seized

Documents (in whatever form) relating to violations of Title 18, United States Code, Sections 2261A (Stalking); 876(c) (Mailing Threatening Communications); 245 (Federally Protected Activities); and 371 (Conspiracy), that is,

1. All documents relating to attempts to locate the home addresses of any members of the media, the Anti-Defamation League, persons who identify as Jewish, or ethnic minorities;

2. All documents relating to the Atomwaffen Division, including members of the group;

3. All documents containing swastikas, other Nazi symbols, or other symbology related to white-supremacist violent extremism;

4. All documents containing the monikers "Krokodil," "Lazarus," "14ALG88," "Azazel," "Roman," "Swissdiscipline," "OldScratch," or "पकजबतचषथबल";

5. All communications with Kaleb Cole;

6. Evidence of who used, owned, or controlled the PHONE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence:

   a. evidence indicating how and when the phone was accessed or used to determine the chronological context of phone access, use, and events relating to crime under investigation and to the phone user;

   b. evidence indicating the phone user's state of mind as it relates to the crime under investigation;

   c. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the phone;

   d. evidence of the times the phone was used;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. passwords, encryption keys, and other access devices that may be necessary to access the phone;

f. documentation and manuals that may be necessary to access the phone or to conduct a forensic examination of the phone;

g. records of or information about Internet Protocol addresses used by the phone;

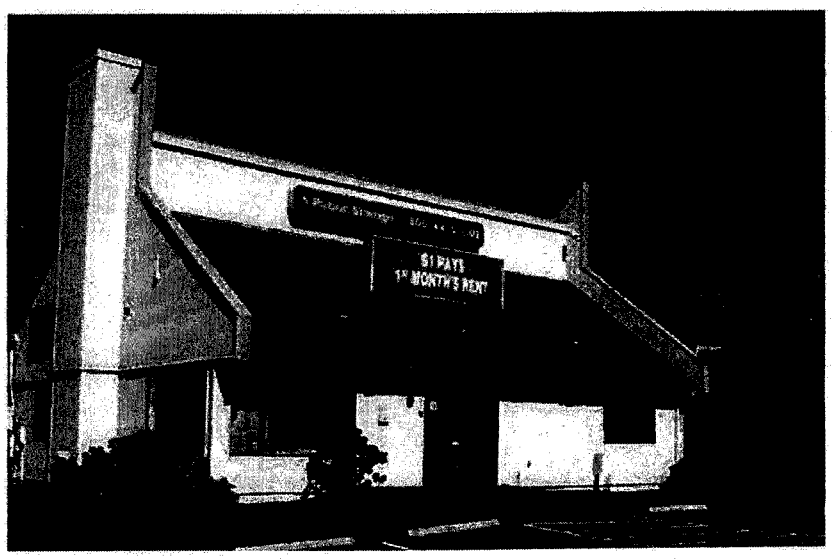
h. records of or information about the phone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

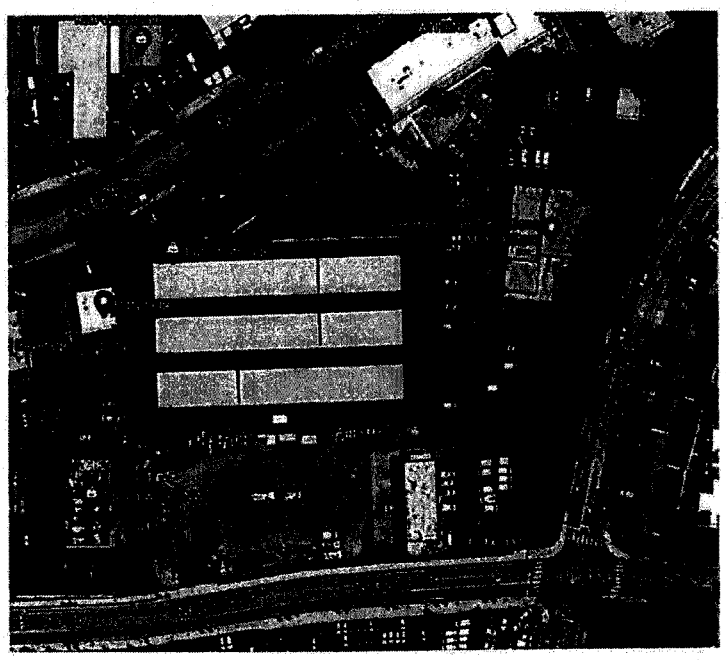
i. contextual information necessary to understand the evidence described in this attachment.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A4
Property to be Searched

The property to be searched is Storage unit # 3348. It is a 5' x 10' storage unit located within the Public Storage at 12425 NE 124th St., Kirkland, WA





UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B4
Property to be Seized

Documents (in whatever form) relating to violations of Title 18, United States Code, Sections 2261A (Stalking); 876(c) (Mailing Threatening Communications); 245 (Federally Protected Activities); and 371 (Conspiracy), that is:

1. All documents relating to attempts to locate the home addresses of any members of the media, the Anti-Defamation League, persons who identify as Jewish, or ethnic minorities;

2. All documents relating to the Atomwaffen Division, including members of the group;

3. All documents containing swastikas, other Nazi symbols, or other symbology related to white-supremacist violent extremism;

4. All stamps, packaging tape, and blank envelopes;

5. All receipts reflecting purchases of stamps, packaging tape, or blank envelopes in January 2020;

6. All documents containing the monikers "Krokodil," "Lazarus," "14ALG88," "Azazel," "Roman," "Swissdiscipline," "OldScratch," or "पकजबतचषथबल";

7. All communications with Kaleb Cole;

8. Digital devices or other electronic storage media and/or their components, which include:

   a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

   b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

   c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

9. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970